UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

VETERINARY IMAGING CENTER OF SAN DIEGO, INC.,	)	
Plaintiff,	)	
v.	)	Civil Action No. 20-10927
JOHN DOES 1-16,	)	
Defendants.	)	

MEMORANDUM OF LAW SUPPORTING PLAINTIFF'S *EX-PARTE* MOTION FOR EMERGENCY DISCOVERY

I. INTRODUCTION

Plaintiff Veterinary Imaging Center of San Diego, Inc., ("Plaintiff") suffered a malicious copyright infringement attack against its copyrighted database, Vetology AI Image Bank (the "Attack"). Plaintiff brings this John Doe matter under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), the Copyright Act, 17 U.S.C. § 102, and the Stored Communications Act, 18 U.S.C. § 2701, to unmask the perpetrators responsible for the Attack, to prevent future attacks, and to hold the Defendants accountable by seeking compensation for the economic damages Plaintiff suffered as a result of Defendants' unlawful and malicious conduct. Unless emergency discovery is granted, however, Plaintiff remains exposed to these same attackers and the information Plaintiff requires to protect itself may be irrevocably lost. Plaintiff also needs the necessary information to identify the Defendants by name in an amended complaint and thereby

prosecute this action. As a result, therefore, and for the reasons contained herein, Plaintiff respectfully requests that the Court grant this *Ex Parte* Motion for Emergency Discovery.

The specific information currently sought is very limited: customer records and any usage logs for a specific date range in the possession of third parties who are the registered owners of Internet Protocol ("IP") addresses that were used in the Attack and any additional IP addresses leased and/or provided by such registered owners to Defendants.

II. FACTUAL BACKGROUND

Over a period of time between November 2019 and March 1, 2020, Defendants used IP addresses located in places all over the world to mass download large portions of VICSD's "Vetology AI Image Bank" database which is protected by a copyright registration on file with U.S. Copyright office. (Complaint ¶ 19, ¶20, 26). This mass downloading was done without the permission of VICSD, and in violation of VICSD's terms of use and its copyright. (*Id.* ¶¶ 15, 19, 21, 22, 25). VICSD believes that this mass downloading is in fact an attempt to steal VICSD's data in an attempt to build a competitive database. (*Id*. ¶ 2, 22). As a result, VICSD has had to suspend its database services for all users, suffering the loss of present and future users that were driven to VICSD's website by the database. (*Id*. ¶ 2, 23, 33). In the process, VICSD has spent significant time and incurred significant expenses in containing the damage caused by the Attack and mitigating further potential damage. (*Id*. ¶ 2, 23, 33).

Immediately after discovering the Attack, VICSD worked to identify the source by tracking down the IP addresses that had mass downloaded VICSD's database; this resulted in a list of IP addresses located all over the world. (*Id*. ¶ 26). Then, VICSD used directories published by ARIN, a third party responsible for managing and distributing IP addresses in the United States, to discover that all of the IP addresses used in the Attack were registered to "IPVanish" a

commercial VPN service based in the United States. (*Id*. ¶ 27). IPVanish is owned and operated by Defendant Mudhook Marketing, Inc., a Florida corporation. (*Id*. ¶ 27). IPVanish is a commercial virtual provide network provider that offers its user a software platform which can mask the user's true IP address by using a decoy IP address located in a different location to take its place. (*Id*. ¶ 28). According to IPVanish's website, that purpose of the software is to allow internet "while your identifying IP address is concealed." (*Id*. ¶ 29).

Plaintiff served IPVanish with a copyright infringement notification on May 5, 2020 pursuant to the Digital Millennium Copyright Act ("DMCA"), relating to the Attack that had occurred on VISCD's database. (*Id*. ¶ 30). In the infringement notification VISCD notified IPVanish that its IP addresses had been used in the Attack in violation of IPVanish's own DMCA policy. (*Id*. ¶ 30) Plaintiff requested that IPVanish stop activity originating from its networks, cease and desist the harmful activity, and contact its users involved in the Attack and inform them to cease and desist as well. (*Id*. ¶ 30). Lastly, Plaintiff requested that IPVanish identify the parties involved in the Attack. (*Id*. ¶ 30). As of now, IPVanish has not responded to this notification or any of Plaintiff's requests at all. Plaintiff also served IPVanish with an abuse report, containing the same information as in the infringement notification, via IPVanish's published abuse reporting email address. (*Id*. ¶ 31). As of now, IPVanish has also not responded to Plaintiff's abuse report.

IPVanish's Privacy Policy states that IPVanish does "not provide information that we do have unless we are legally required to." (Ex. C to Affidavit of J. Mark Dickison, IPVanish's Privacy Policy pg. 6). IPVanish's policy of not providing information to third parties unless forced to explains the lack of response that the Plaintiff has received. It seems clear that

IPVanish will not cooperate with any of the Plaintiff's requests unless they are legally mandated to do so.

In sum, Plaintiff's request is critical to identifying the wrongdoers and also to maintaining a strong defense against any other attacks by Defendants in the future. If Plaintiff has a list of the IP addresses that IPVanish provide to Defendants, it can more effectively block all traffic originating from Defendants and thus prevent another attack where Defendants would be able to steal Plaintiff's entire database. Furthermore, Plaintiff's request will allow it to further investigate the identities of the Defendants and effectively pursue its CFAA, Copyright Act, and Store Communications Act claims against them.

It is critical that this discovery proceed immediately, because subscriber logs are often retained for only short periods of time. Moreover, the unknown Defendants previously used IPVanish IP addresses for the Attack. Until Plaintiff is able to block all the IP addresses IPVanish provides to the Defendants, Plaintiff will be unable to reopen its database for public use out of the likely result that the Defendants would recreate another attack, causing VICSD ever more harm. (*See*, *id*. ¶¶ 23, 33).

III. ARGUMENT

A. The Federal Rules Allow For Emergency Discovery

District Courts have broad power to require emergency document production and to permit expedited discovery. *See* Fed. R. Civ. P. 26(f), 30(b), 34(b). Courts may grant expedited discovery when the movant has made a showing of good cause. *London-Sire Records, Inc. v. Doe 1*, 542 F.Supp.2d 153, 164 (D. Mass. 2008), *McMann v. Doe*, 460 F. Supp. 2d 259, 265 (D. Mass. 2006). Courts consider the following factors when granting motions for expedited discovery to identify anonymous Internet users: (1) a concrete showing of a prima facie claim of

actionable harm, (2) specificity of the discovery requests, (3) the absence of alternative means to obtain the subpoenaed information, (4) a central need for the subpoenaed information to advance the claim, and (5) the party's expectation of privacy. *See Sony Music Enter. Inc. v. Does 1–40*, 326 F.Supp.2d 556, 564–65 (S.D.N.Y. 2004) *followed by London-Sire Records, Inc.*, 542 F.Supp.2d at 164, n.13 (collecting authorities that have followed the *Sony Music* standard).

B. Plaintiff Presents A Prima Facie Case Of A Violation Of The Computer Fraud And Abuse Act, 18 U.S.C. § 1030

The CFAA prohibits, among other things, "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer." 18 U.S.C. § 1030(a)(5)(A). The CFAA specifically allows "any person who suffers damage or loss" from a violation of the CFAA to bring a civil action against the violator so long as one of five types of conduct is alleged, including loss to one or more persons during any 1-year period aggregating at least $5,000 in value. 18 U.S.C. § 1030(g); *see also* 18 U.S.C. § (c)(4)(A)(i)(I).

Plaintiff's allegations make a prima facie case for a violation of the CFAA. Plaintiff alleges that Defendants' knowingly used decoy IP addresses to infiltrate Plaintiff's website and attempted to mass download Plaintiff's entire database. (Complaint ¶¶ 20-23, 25-29). Plaintiff's website is a protected computer under 18 U.S.C. § 1030 and the attack caused more than $5,000 in damages. (Complaint ¶¶ 37-40, 42). These allegations are legally-sufficient and grounded in concrete facts rendering emergency discovery appropriate. *See London-Sire*, 542 F. Supp. 2d at 164-675 ("[The] standard does not require the plaintiffs to prove their claim. They need only to proffer sufficient evidence that, if credited, would support findings in their favor.").

C. Plaintiff Presents A Prima Facie Case Of A Violation Of The Copyright Act, 17 U.S.C. § 102

To state a prima facie claim of copyright infringement, the Plaintiff must show "(1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original." *Johnson v. Gordon*, 409 F.3d 12, 17 (1st Cir.2005) (quoting *Feist Publ'ns, Inc. v. Rural Tel. Service Co., Inc.*, 499 U.S. 340, 361 (1991)). For the first element, a copyright registration certificate for the claimed work is prima facie evidence of valid ownership. *See*, *Situation Mgmt. Sys., Inc. v. ASP. Consulting LLC*, 560 F.3d 53, 58 (1st Cir. 2009). 17 U.S.C. § 410(c). The second element has two components. First, the Plaintiff must establish that the infringer copied the protected work. *Soc'y of Holy Transfiguration Monastery, Inc. v. Gregory*, 689 F.3d 29, 48 (1st Cir. 2012). And second, that the copying was so flagrant that the works are "substantially similar". *Id*. at 48.

Plaintiff's allegations make a prima facie case for a violation of copyright infringement. Plaintiff has adequately alleged that it is a valid copyright owner of the works. (Complaint ¶¶ 17-19, 52). Plaintiff has also submitted a Certificates of Registration issued by the U.S. Copyright Office, as prima facie evidence that it is a valid copyright owner. (Ex. A to Affidavit of J. Mark Dickison, Email concerning issuance of Certificate of Registration No. TX 8-865-894). Plaintiff has also adequately alleged that the Defendants have copied the original works by showing that Defendants both had access and did access the works, and that the Defendant copied the works directly by downloading the entirety of the Plaintiff's database. (Complaint ¶¶ 20-26, 53-54). The works are substantially similar because the database was downloaded directly. (*Id.* ¶¶ 20, 53-54). These allegations are legally-sufficient and grounded in concrete facts rendering emergency discovery appropriate. *See London-Sire*, 542 F. Supp. 2d at 164-675.

D. Plaintiff Presents A Prima Facie Case Of A Violation Of The Stored Communications Act, 18 U.S.C. § 2701

The Stored Communications Act defines an offense as when anyone "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system". 18 U.S.C. § 2701(a). The Stored Communications Act also creates a private cause of action for aggrieved providers

> **(a) Cause of action.**--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

18 U.S.C. § 2707(a). In such a civil action, the statute defines appropriate relief as "preliminary" or "declaratory relief", "damages", and "reasonable attorney's fee and other litigation costs". 18 U.S.C. § 2707(b).

Plaintiff's allegations make a prima facie case for a violation of the Stored Communications Act. The Plaintiff has adequately alleged that the Defendant either accessed the facility without authorization, or exceeded his authorization, and obtained access to an electronic communication in violation of the statute. Plaintiff alleges that Defendants' knowingly used decoy IP addresses to infiltrate Plaintiff's website and attempted to mass download Plaintiff's entire database. (Complaint ¶¶ 20-26, 33-34). In doing so, Defendant knowingly violated Plaintiff's Terms of Use and accessed the Plaintiff's database without proper authorization. (*Id*. ¶¶ 15, 20-22, 25, 45-48). The Defendant thereby obtained a copy of the Plaintiff's database and prevented authorized access to the database in violation of the statute. (*Id*. ¶¶ 20, 23, 50). These allegations are legally-sufficient and grounded in concrete facts rendering emergency discovery appropriate. *See London-Sire*, 542 F. Supp. 2d at 164-675.

E. Plaintiff's Discovery Requests Are Reasonably Specific

Plaintiff's personnel identified the IP addresses responsible for the Attack and a third party, ARIN, through its public directories, confirmed that the third party, IPVanish, was the source of the IP addresses used in the Attack. (Complaint ¶ 27).

Plaintiff's proposed subpoena is narrowly-focused and reasonably specific. Plaintiff's goal is to discover the identity of the Defendants and prevent a future attack. (*See* Affidavit of J. Mark Dickison in Support of Motion for Emergency Discovery, Ex. D, Subpoena Template). Plaintiff's proposed subpoena would require IPVanish to provide only the complete customer information relating to a small number of IP addresses. The discovery only requires IPVanish to reveal information with respect to individuals and/or companies related to the Attack, and it does not require the third parties to reveal the content of any communications. The requested information, however, will establish forensically the source of the Attack. Indeed, the information Plaintiff seeks has been found to be appropriately discoverable in analogous situations. *See London-Sire*, 542 F. Supp. 2d at 178 and n.34 (early discovery of identifying information was appropriate and noting that Media Access Control ("MAC") addresses are "highly probative").

F. The Identity Of The John Does And The Other IP Addresses They Might Use Are Central To Plaintiff's Ability To Protect Itself, And It Cannot Otherwise Obtain This Information.

There can be little dispute that Plaintiff meets the requirements of prongs three (the absence of alternative means to obtain the subpoenaed information) and four (a central need for

the subpoenaed information to advance the claim) of the *Sony Music* test. Plaintiff has made requests for IPVanish and others to provide the requested identifying information without a subpoena. Plaintiff has already exhausted practically all non-judicial means of obtaining additional information from IPVanish and does not expect other third parties to be more forthcoming with the requested information. (Complaint ¶¶ 30-32). Without this additional information from IPVanish Plaintiff cannot continue to investigate the identity of the Defendants or fully protect itself from future attacks. Expedited discovery is often the only way to gain the information necessary to move the case forward. *See e.g.*, *London-Sire*, 542 F.Supp.2d at 179 (noting litigation cannot progress without further information regarding the Doe defendants); *Sony Music*, 326 F.Supp.2d at 566 (holding that prongs three and four were met in an analogous copyright infringement suit against anonymous users of a peer-to-peer network). Thus, discovery and subpoenas to third party IP address registrants like IPVanish is necessary for Plaintiff to prosecute this action.

G. The John Does Have No Expectation Of Privacy In This Instance

The Defendants' expectations of privacy turn upon the Privacy Policies and Acceptable Use Policies that govern their use of various internet services such as IPVanish. *See e.g.*, *London-Sire*, 542 F. Supp. 2d at 179 (noting that, in the context of copyright litigation, internet service providers may require their customers to acknowledge as a condition of service they are forbidden from engaging in copyright infringement and have no privacy rights for such actions). Here, IPVanish's Acceptable Use Policy, located in its Terms of Service states customers

> "[M]ay not use our Services, or our Software or System, to post or transmit any illegal material, including without limitation any transmissions that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, state, national or international law or regulation."

(Ex. B to Affidavit of J. Mark Dickison, IPVanish's Terms of Service ¶ 12). It also prohibits "[t]ransmitting or receiving, uploading, using or reusing material that violates any intellectual property rights of a third party, including, without limitation, patent, trademark or copyrights" (*Id.* ¶ 12). More explicitly, IPVanish states in its Terms of Service that

> IPVanish respects the intellectual property rights of others and expects that you do the same. It is our policy to terminate in appropriate circumstances the accounts of subscribers who infringe the copyrights of others. You may not upload, download, post, publish, transmit, reproduce, or distribute in any way, files, material, information, software or other material obtained through the System that is protected by copyright or other proprietary right or derivative works with respect thereto, without obtaining permission of the copyright owner or other right holder. Additionally, you shall not upload, download, post, publish, reproduce, transmit or distribute in any way any component of the System itself or derivative works with respect thereto.

(Id. ¶ 13). Plaintiff expects that additional discovery will likely show similar provisions in all applicable Terms of Service, Privacy Policies, and Acceptable Use Policies.

A copyright infringement attack caused by illegally downloading media is a black-letter violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the Copyright Act, 17 U.S.C. § 102, and the Stored Communications Act, 18 U.S.C. § 2701. *See Viiken Detection Corporation; Peter Rothschild V. John Doe*, No. 19-cv-12034-NMG. (D. Mass. October 17, 2019) (granting motion for leave to issue third part subpoenas for plaintiffs that alleged violations of the CFAA and the Stored Communications Act for illegally downloaded documents). Thus, at a minimum the Defendant's use of the IP addresses registered to IPVanish to perpetrate such an attack clearly violates IPVanish's Acceptable Use Policy as it involved transmissions in violation of copyright law. (Dickison Affidavit. Ex. E). Thus, Defendants have no expectation of privacy under IPVanish's Privacy Policy in the customer data Plaintiff seeks and likely have no similar expectation for their interactions with the other third party IP address registrants.

IV. CONCLUSION

Plaintiff has shown good cause for emergency discovery to identify Defendants and protect itself from future infringement. Defendants have violated the CFAA by stealing content from Plaintiff's website, and Plaintiff's proposed discovery requests are specifically focused on identifying the Defendants and preventing future infringement. Plaintiff is unable to obtain this information without a subpoena for the overwhelming majority of the Defendants' IP addresses. This information is critical to Plaintiff's ability to protect itself and identify the Defendants so that it can adequately prosecute this action. Lastly, Defendants have no expectation of privacy as their actions violate applicable acceptable use policies and federal law. Plaintiff thus respectfully requests that the Court authorize emergency discovery in this matter.

Dated: May 14, 2020

Respectfully submitted,

/s/ J. Mark Dickison
J. Mark Dickison (BBO #629170)
John R. Bauer (BBO #630742)
LAWSON & WEITZEN, LLP
88 Black Falcon Avenue
Boston, MA 02210
Telephone (617) 439-4990
Facsimile (617) 439-3987
mdickison@lawson-weitzen.com
jbauer@lawson-weitzen.com